Theoretical Computer Science 412 (2011) 4592–4603

Contents lists available at ScienceDirect

Theoretical Computer Science

journal homepage: www.elsevier.com/locate/tcs

Applying IsRewritten criterion on Buchberger algorithm

Amir Hashemi *, Benyamin M.-Alizadeh

Department of Mathematical Sciences, Isfahan University of Technology, Isfahan, 84156-83111, Iran

ARTICLE INFO

Article history:
Received 22 June 2010
Received in revised form 18 January 2011
Accepted 23 April 2011
Communicated by G. Ausiello

Keywords:
Gröbner bases
Buchberger's algorithm
IsRewritten criterion

ABSTRACT

Faugère's F_5 algorithm is one of the fastest algorithms to compute Gröbner bases. It uses two criteria namely the F_5 criterion and the IsRewritten criterion to detect the useless critical pairs (see Faugère (2002) [8]). The IsRewritten criterion has been used in the F_5 algorithm, but it has not been explicitly declared in the related paper. In this paper, we give first a complete proof for the IsRewritten criterion and then using a signature structure on Buchberger's algorithm, we apply this criterion on Buchberger's algorithm. We have implemented a new algorithm (based on the above results) in MAPLE to compute a Gröbner basis of a general ideal and we evaluate its performance via some examples.

0. Introduction

One of the most important tools in computational algebraic geometry is the *Gröbner basis*. This concept and the first algorithm, were introduced in 1965 by Buchberger in his Ph.D. thesis (see [3]). His two criteria and the implementation methods (see [4,5]) made the Gröbner basis a powerful tool to solve many important problems in polynomial ideals theory. But Buchberger's algorithm is very time-consuming for large polynomial systems, therefore it is not efficient in practice.

In 1983, Lazard described a new algorithm to compute Gröbner bases. This algorithm was faster than Buchberger's algorithm because it used linear algebra techniques (see [12]). In 1988, Gebauer and Möller installed Buchberger's two criteria on Buchberger's algorithm in an essential way (see [10]). In 1994, Faugère described his F_4 algorithm to compute Gröbner bases (see [7]). This algorithm is an efficient algorithm which forms a generally sparse matrix and uses fast linear algebra. This algorithm was implemented in some computer algebra systems such as MAPLE and MAGMA.

In 2002, following Möller et al.'s idea (see [13]), Faugère described F_5 (see [8]), a new incremental algorithm to compute Gröbner bases. The cornerstone of the F_5 algorithm was based on two criteria, known as the F_5 criterion and the IsRewritten criterion. It is worth noting that the IsRewritten criterion has been used in the F_5 algorithm, however it has not been explicitly declared in [8]. This criterion is a non-matrix representation of the simplification sub-algorithm in the F_4 algorithm (see [7]). These criteria are based on the concept of the "signature" of a polynomial and the ordering defined on the signatures (see Section 1).

Ars and Hashemi in [1] have proposed a non-incremental version of the F_5 algorithm. They have defined a new ordering on the signatures to make F_5 independent from the order of input polynomials. Eder and Perry (see [6]) have simplified some of the steps in the F_5 algorithm, by computing the reduced Gröbner basis at each step of the algorithm (this algorithm, called F_5C, is faster than F_5). Gao et al. in [9] have presented a new incremental algorithm in the same method as F_5C and F_5 which

* Corresponding author. Tel.: +98 31 13 91 36 35; fax: +98 31 13 91 26 02.
E-mail addresses: Amir.Hashemi@cc.iut.ac.ir (A. Hashemi), B.Alizadeh@math.iut.ac.ir (B. M.-Alizadeh).

0304-3975/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2011.04.040

is more efficient than these algorithms. Recently, Sun and Wang in [14] have described the F_5 algorithm in Buchberger's style (F_5B algorithm), where both the F_5 criterion and the IsRewritten criterion are applied. However, in F_5B, they have not combined these criteria with Buchberger's two criteria.

In this paper, we first present a complete proof for the IsRewritten criterion and then using a signature structure on Buchberger's algorithm, we apply this criterion on Buchberger's algorithm. In fact, we give a theoretical and practical answer to the question about how Buchberger's criteria with the IsRewritten criterion in Buchberger's algorithm can be combined. We have implemented a new algorithm (based on the above results) in MAPLE to compute the Gröbner basis of a general ideal and we evaluate its performance via some examples.

Now, we give the structure of the paper. In Section 1, we present briefly the theory behind the F_5 algorithm. In Section 2, we define the IsRewritten criterion and we give a complete proof for it. In Section 3, we explain the relationship between the IsRewritten criterion and Buchberger's criteria. Section 4 is devoted to the description of our algorithm, which applies the IsRewritten criterion on Buchberger's algorithm. In Section 5, we prove the correctness of this algorithm. In Section 6, we show the performance of our algorithm with respect to our implementation of the improved Buchberger's algorithm via some examples.

1. Faugère's F_5 algorithm

This section aims to present the theory behind the F_5 algorithm. After recalling some notations and definitions (used also in the next sections), the principal theorem which forms the basis of the F_5 algorithm is stated (we refer to [8] for more details).

Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring, where K is an arbitrary field and $I = \langle f_1, \ldots, f_k\rangle$ be an ideal of R generated by the homogeneous polynomials $f_1, \ldots, f_k$. Let $f \in R$ and $<$ be a monomial ordering on R. The *leading monomial* of f is the greatest monomial (with respect to $<$) which appears in f, and we denote it by $\mathrm{LM}(f)$. The *leading coefficient* of f, written $\mathrm{LC}(f)$, is the coefficient of $\mathrm{LM}(f)$ in f. The *leading term* of f is $\mathrm{LT}(f) = \mathrm{LC}(f)\mathrm{LM}(f)$. The *leading term ideal* of I is defined as

$$\mathrm{LT}(I) = \langle \mathrm{LT}(f) \mid f \in I\rangle.$$

Let R^k be an k-dimensional R-module and let $\mathbf{f_1}, \ldots, \mathbf{f_k}$ be its canonical basis. Thus, a module monomial is of the form $m\mathbf{f_i}$ where $m \in R$ is a monomial. We can extend $<$ to a module monomial ordering on R^k by the following definition:

$$\sum_{i=j}^{k} g_i\mathbf{f_i} \prec \sum_{i=\ell}^{k} h_i\mathbf{f_i} \quad \text{iff} \quad \begin{cases} j > \ell & \text{and} \quad h_\ell \neq 0 \text{ or} \\ j = \ell & \text{and} \quad \mathrm{LM}(g_j) < \mathrm{LM}(h_j). \end{cases}$$

For an element $\mathbf{g} = \sum_{i=1}^{k} g_i\mathbf{f_i} \in R^k$, we define the index of $\mathbf{g}$, $\mathrm{index}(\mathbf{g})$ to be the lowest integer i such that $g_i \neq 0$. Let $\mathrm{index}(\mathbf{g}) = i_0$, then we call $\mathrm{LM}(g_{i_0})\mathbf{f_{i_0}}$ the *module leading monomial* of $\mathbf{g}$ and denote it by $\mathrm{MLM}(\mathbf{g})$. Also we use $\mathrm{LM}(\mathbf{g})$ to denote $\mathrm{LM}(\sum_{i=1}^{k} g_i f_i)$.

In the following, we recall the definition of the signature of a polynomial. This is a unique data however not dependent on the order of the computation. To store it, we need to represent a polynomial in $A = R^k \times R$. An element of A is called a *labeled* polynomial; if it is of the form $(m\mathbf{f_i}, f)$ where m is a monomial, i is some integer and f is a polynomial. For a labeled polynomial $r = (m\mathbf{f_i}, f) \in A$, we define its *polynomial part* by $\mathrm{poly}(r) = f$ and its *signature* by $\mathcal{S}(r) = m\mathbf{f_i}$. It is possible, this additional machinery models the polynomials in such a way to make use of additional data during F_5. In fact, it permits the algorithm to ignore full normal form reduction of polynomials, done during Buchberger's algorithm.

A labeled polynomial $r = (\mathcal{S}(r), \mathrm{poly}(r))$ is called *admissible* if there exists $\mathbf{g} \in R^k$ such that $\psi(\mathbf{g}) = \mathrm{poly}(r)$ and $\mathrm{MLM}(\mathbf{g}) = \mathcal{S}(r)$ where $\psi : R^k \to R$ is a map so that

$$\psi\,(g_1, \ldots, g_k) = g_1 f_1 + \cdots + g_k f_k$$

where g_i's are polynomials in R. We define the following operations on labeled polynomials: Let $r = (m\mathbf{f_i}, f)$ be a labeled polynomial, u be a monomial and c be a constant. Then, we define $ur = (um\mathbf{f_i}, uf)$ and $cr = (m\mathbf{f_i}, cf)$. These definitions and a special reduction of F_5 ensure that during a Gröbner basis computation by F_5, it takes the minimal possible signature for an admissible labeled polynomial.

It needs more definitions to state the main theorem of [8].

Definition 1.1 (F_5 *Criterion*)**.** An admissible labeled polynomial $r = (m\mathbf{f_i}, f)$ is called *normalized* if $m \notin \mathrm{LM}(\langle f_{i+1}, \ldots, f_k\rangle)$. A pair (r, s) of admissible labeled polynomials is normalized if ur and vs are normalized where $r = (m\mathbf{f_i}, f)$, $s = (m'\mathbf{f_j}, g)$, $u = \frac{\mathrm{lcm}(\mathrm{LM}(f),\mathrm{LM}(g))}{\mathrm{LM}(f)}$ and $v = \frac{\mathrm{lcm}(\mathrm{LM}(f),\mathrm{LM}(g))}{\mathrm{LM}(g)}$.

Faugère has described F_5 as an incremental algorithm to use F_5 criterion, i.e. to compute the Gröbner basis of I, it computes the Gröbner bases of the ideals generated by

$$\{f_k\}, \{f_{k-1}, f_k\}, \ldots, \{f_1, \ldots, f_k\}.$$

In the following, we define the concept of t-representation for labeled polynomials, imposing additional conditions on the signatures (see [2], page 219).

Definition 1.2. Let $P \subset A$ be a finite set of labeled polynomials, and $r, t \in A$ be two labeled polynomials with $\text{poly}(r) = f$, where $f \neq 0$. We say that

$$f = \sum_{p_i \in P} h_i \text{poly}(p_i)$$

is a *t-representation* of r w.r.t. P if for all $p_i \in P$ with $\text{poly}(p_i) \neq 0$ we have

$$\text{LM}(h_i)\text{LM}(\text{poly}(p_i)) \preceq \text{LM}(\text{poly}(t)) \quad \text{and} \quad \text{LM}(h_i)\mathcal{S}(p_i) \preceq \mathcal{S}(r).$$

This property is denoted by $r = \mathcal{O}_P(t)$. We write $s = o_P(t)$ if there exists a labeled polynomial $t' \in A$ satisfying $\mathcal{S}(t') \preceq \mathcal{S}(t)$ and $\text{LM}(poly(t')) \prec \text{LM}(poly(t))$ such that $s = \mathcal{O}_P(t')$.

Let $f, g \in R$ be two polynomials. The *S-polynomial* of f and g is defined as:

$$\text{Spoly}(f, g) = \frac{\text{lcm}(\text{LM}(f), \text{LM}(g))}{\text{LT}(f)} f - \frac{\text{lcm}(\text{LM}(f), \text{LM}(g))}{\text{LT}(g)} g.$$

Let $r = (\mathcal{S}(r), f)$ and $s = (\mathcal{S}(s), g)$ be two admissible labeled polynomials such that $v\mathcal{S}(s) \prec u\mathcal{S}(r)$ with $u = \frac{\text{lcm}(\text{LM}(f),\text{LM}(g))}{\text{LM}(f)}$ and $v = \frac{\text{lcm}(\text{LM}(f),\text{LM}(g))}{\text{LM}(g)}$. Then, we define $\text{Spoly}(r, s) = (u\mathcal{S}(r), \text{Spoly}(f, g))$.

Theorem 1.1 (*[8]*). *Let $I = \langle f_1, \ldots, f_k \rangle$ be an ideal of $R = K[x_1, \ldots, x_n]$. Let $G \subset A = R^k \times R$ be a finite set of admissible labeled polynomials such that*

- *For every i, we have $f_i = \text{poly}(r_i)$ for some $r_i \in G$.*
- *For each $(r_i, r_j) \in G \times G$ which is normalized, $\text{Spoly}(r_i, r_j)$ is either zero or equal to $o_G(u_s r_s)$ where $u_s = \frac{\text{lcm}(\text{LM}(\text{poly}(r_i)),\text{LM}(\text{poly}(r_j)))}{\text{LM}(\text{poly}(r_s))}$ for $s \in \{i, j\}$.*

Then the set $\{\text{poly}(r) \mid r \in G\}$ is a Gröbner basis for I.

2. IsRewritten criterion

In this section we first define the IsRewritten criterion and then we prove it (this criterion has not been explicitly declared, not proved in [8], however it has been used in the F_5 algorithm). Our definition of the IsRewritten criterion is based on the module monomial ordering defined in the previous section.

Definition 2.1 (*IsRewritten Criterion*)**.** With the notation of the previous section, let $u \in R$ be a monomial and $r = (m\mathbf{f_i}, f)$ be an admissible labeled polynomial. Then, the pair $[u, r]$ is called *rewritable* if there exists an admissible labeled polynomial $r' = (m'\mathbf{f_i}, f')$ computed after r, that is $\mathcal{S}(r) \prec \mathcal{S}(r')$, such that m' divides um. A pair (r, s) of admissible labeled polynomials is rewritable if $[u, r]$ or $[v, s]$ is rewritable where $r = (m\mathbf{f_i}, f), s = (m'\mathbf{f_j}, g), u = \frac{\text{lcm}(\text{LM}(f),\text{LM}(g))}{\text{LM}(f)}$ and $v = \frac{\text{lcm}(\text{LM}(f),\text{LM}(g))}{\text{LM}(g)}$.

As the following proposition yields, if a critical pair is rewritable, its S-polynomial has a standard representation with respect to the last computed Gröbner basis, and therefore the F_5 algorithm deletes all such pairs. It is worth noting that the IsRewritten criterion is not related to the F_5 criterion.

Proposition 2.1. *Let $I = \langle f_1, \ldots, f_k \rangle \subset R$ be an ideal. Let r_i and r_j be two labeled polynomials treated during an execution of the F_5 algorithm for computing the Gröbner basis of I. If (r_i, r_j) is rewritable then $\text{Spoly}(r_i, r_j)$ is either zero or equal to $o_G(u_s r_s)$ where $u_s = \frac{\text{lcm}(\text{LM}(\text{poly}(r_i)),\text{LM}(\text{poly}(r_j)))}{\text{LM}(\text{poly}(r_s))}$ for $s \in \{i, j\}$ (and therefore the pair (r_i, r_j) can be eliminated).*

Proof. Let $\text{Spoly}(r_i, r_j) \neq 0$. Wlog, suppose that (u_i, r_i) is rewritable. From Definition 2.1, there exists an admissible labeled polynomial r_m such that $u_i\mathcal{S}(r_i) = u_m\mathcal{S}(r_m)$ for some monomial u_m. Let $\text{poly}(r_i) = \sum_{h=\ell}^{k} p_h f_h$ and $\text{poly}(r_m) = \sum_{h=\ell}^{k} q_h f_h$

where index$(r_i) = \ell$. From the hypothesis, $u_i\mathrm{LM}(p_\ell) = u_m\mathrm{LM}(q_\ell)$ and we can write:

$$\begin{aligned}
u_i\mathrm{poly}(r_i) &= u_i \sum_{h=\ell}^{k} p_h f_h \\
&= u_i p_\ell f_\ell + u_i \sum_{h=\ell+1}^{k} p_h f_h \\
&= u_i(\mathrm{LM}(p_\ell) + \mathrm{tail}(p_\ell))f_\ell + u_i \sum_{h=\ell+1}^{k} p_h f_h \\
&= (u_m(q_\ell - \mathrm{tail}(q_\ell)) + u_i\mathrm{tail}(p_\ell))f_\ell + u_i \sum_{h=\ell+1}^{k} p_h f_h \\
&= u_m q_\ell f_\ell + (u_i\mathrm{tail}(p_\ell) - u_m\mathrm{tail}(q_\ell))f_\ell + u_i \sum_{h=\ell+1}^{k} p_h f_h \\
&= u_m\mathrm{poly}(r_m) + (u_i\mathrm{tail}(p_\ell) - u_m\mathrm{tail}(q_\ell))f_\ell + \sum_{h=\ell+1}^{k} (u_i p_h - u_m q_h)f_h. \qquad (1)
\end{aligned}$$

Form (1), it follows that instead of computing Spoly(r_i, r_j), we may replace some calculated S-polynomials between $r_j, r_m, f_\ell, \ldots, f_k$. All these S-polynomials have been (will be) studied during the execution of the F_5 algorithm for computing the Gröbner basis of I and they have (will have) a standard representation. But, we first have to prove that replacing the S-polynomials between $r_m, f_\ell, \ldots, f_k$ does not create a loop. Otherwise, we omit the pair (r_i, r_j) referring to itself which makes the algorithm go wrong. Let $u_i r_i = u\mathrm{Spoly}(r_m, r)$ for some monomial u and some labeled polynomial r. We consider the following two cases:

- if $u = 1$, we can study Spoly$(r_j, \mathrm{Spoly}(r_m, r))$ instead of Spoly(r_i, r_j). The polynomial Spoly(r_m, r) will be constructed further and it is not equal to r_i, because $\mathcal{S}(r_i) \prec \mathcal{S}(r_m)$.
- if $u \neq 1$, then $\mathcal{S}(\mathrm{Spoly}(r_m, r)) = u_i m/u\mathbf{f_i}$. On the other hand, from

  $$\mathrm{lcm}(\mathrm{LM}(\mathrm{poly}(r_m)), \mathrm{LM}(\mathrm{poly}(r))) < \mathrm{lcm}(\mathrm{LM}(\mathrm{poly}(r_i)), \mathrm{LM}(\mathrm{poly}(r_j)))$$

  we can conclude that the pair (r_m, r) has been studied (after r_m and) before (r_i, r_j), note that the polynomials are assumed to be homogeneous. Therefore, the pair (r_i, r_j) is rewritable by the labeled polynomial Spoly(r_m, r) which is a contradiction, because by the structure of the F_5 algorithm, if $[u_i, r_i]$ is rewritable by r_m, this means that r_m is the last polynomial computed after r_i such that $\mathcal{S}(r_m) \mid u_i\mathcal{S}(r_i)$.

To complete the proof, we have to prove that if we replace $u_i r_i$ by (1), no other loop can be formed in Spoly$(r_i, r_j) = u_i r_i + u_j r_j$ (for simplification we do not care about the coefficients). From this we mean that computing Spoly(r_i, r_j) may refer to, for example, Spoly(r_j, r) for some polynomial r. So, if (r_j, r) is rewritable by r_i (let $[u, r]$ be rewritable where $u = \frac{\mathrm{lcm}(\mathrm{LM}(\mathrm{poly}(r_j)),\mathrm{LM}(\mathrm{poly}(r)))}{\mathrm{LM}(\mathrm{poly}(r))}$) then computing Spoly$(r_j, r)$ may refer to Spoly(r_i, r_j) which has been eliminated, and this creates a loop. We prove that this cannot happen. Using reductio ad absurdum, assume that $[u, r]$ is rewritable by r_i. This implies that $u_i'\mathcal{S}(r_i) = u\mathcal{S}(r)$ for some monomial u_i'. It is clear that $r \neq r_m$, because $[u_m, r_m]$ cannot be rewritable by r_i. We can then deduce that Spoly(r_j, r) for some labeled polynomial r forms in (1) where $u\mathrm{poly}(r)$ for some monomial u appears in

$$(u_i\mathrm{tail}(p_\ell) - u_m\mathrm{tail}(q_\ell))f_\ell + \sum_{h=\ell+1}^{k} (u_i p_h - u_m q_h)f_h.$$

Thus, $u_i' r_i$ (instead of $u_i r_i$) should appear in Spoly(r_j, r) (or equivalently in Spoly(r_i, r_j)) which is a contradiction because $u_i'\mathcal{S}(r_i) = u\mathcal{S}(r) \prec u_i\mathcal{S}(r_i)$. □

3. IsRewritten criterion versus Buchberger's criteria

In this section, we state some results clarifying the relationship between the IsRewritten criterion and Buchberger's criteria. It shows some useless critical pairs detected by Buchberger's criteria, may be detected by the IsRewritten criterion. This illustrates the importance and difficulty of combining the IsRewritten criterion with Buchberger's criteria.

Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring, where K is an arbitrary field.

Lemma 3.1 (*Buchberger's First Criterion*). *Let $f, g \in R$ be two polynomials such that* $\operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(g)) = \operatorname{LM}(f)\operatorname{LM}(g)$. *Then,* $\operatorname{Spoly}(f, g)$ *is reduced to zero modulo* $\{f, g\}$.

Proof. See [2], Lemma 5.66 page 222. □

Lemma 3.2. *Let $r = (m\mathbf{f}_i, f)$ and $s = (m'\mathbf{f}_j, g)$ be two admissible labeled polynomials which have been added to the Gröbner basis G during a run of F_5. Also let* $\operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(g)) = \operatorname{LM}(f)\operatorname{LM}(g)$. *Then, the pair (r, s) is either not normalized or rewritable, or* $\operatorname{Spoly}(r, s) = o_{\{r,s\}}(\operatorname{LM}(g)r)$.

Proof. By hypothesis and definition of notations, the signature of $\operatorname{Spoly}(r, s)$ is $max_{\prec}\{\operatorname{LM}(g)m\mathbf{f}_i, \operatorname{LM}(f)m'\mathbf{f}_j\}$. Wlog, we can suppose that $i \leq j$. So, two cases are possible: If $i < j$, this signature is equal to $\operatorname{LM}(g)m\mathbf{f}_i$, and therefore (r, s) is not normalized because $\operatorname{LM}(g)$ divides $\operatorname{LM}(g)m\mathbf{f}_i$ (see F_5 criterion). If $i = j$, then two following cases are possible: Let $\operatorname{LM}(g)m\mathbf{f}_i = \operatorname{LM}(f)m'\mathbf{f}_j$. Since $\operatorname{LM}(f)$ and $\operatorname{LM}(g)$ are disjoint, then $m \neq m'$. Assume that $m < m'$. It follows that $[\operatorname{LM}(g), r]$ is rewritable. Thus, the pair (r, s) is rewritable by the Rewritten criterion. As the last case, if $\operatorname{LM}(g)m\mathbf{f}_i \neq \operatorname{LM}(f)m'\mathbf{f}_j$, the assertion can be deduced from Lemma 3.1.

Corollary 3.1. *Let $r = (m\mathbf{f}_i, f)$ and $s = (m'\mathbf{f}_j, g)$ be two admissible labeled polynomials such that* $\operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(g)) = \operatorname{LM}(f)\operatorname{LM}(g)$. *If (r, s) is normalized and not rewritable then it is a useless pair which cannot be detected by the F_5 criteria.*

Now, we survey Buchberger's second criterion.

Lemma 3.3 (*Buchberger's Second Criterion*). *Let $F \subset R$ be a finite set and $p, f_1, f_2 \in R$ such that the following hold for $i = 1, 2$:*

- $\operatorname{LM}(p)$ *divides* $\operatorname{lcm}(\operatorname{LM}(f_1), \operatorname{LM}(f_2))$.
- $\operatorname{Spoly}(p, f_i)$ *has a t_i-representation w.r.t. F with* $t_i < \operatorname{lcm}(\operatorname{LM}(p), \operatorname{LM}(f_i))$.

Then, $\operatorname{Spoly}(f_1, f_2)$ *has a t-representation w.r.t. F for some monomial* $t < \operatorname{lcm}(\operatorname{LM}(f_1), \operatorname{LM}(f_2))$.

Proof. See [2], Proposition 5.70 page 223. □

Lemma 3.4. *Let $r = (m\mathbf{f}_i, f)$, $s = (m'\mathbf{f}_j, g)$ and $t = (m''\mathbf{f}_\ell, h)$ be three admissible labeled polynomials which have been added to the Gröbner basis G during a run of F_5. Furthermore, assume that* $\operatorname{LM}(h)$ *divides* $\operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(g))$ *and both the pairs (r, t) and (s, t) have already been treated. Let*

$$wm''\mathbf{f}_\ell \preceq \max_{\prec}\{um\mathbf{f}_i, vm'\mathbf{f}_j\}$$

where $\operatorname{Spoly}(f, g) = uf - vg$ *and* $w = \frac{\operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(g))}{\operatorname{LM}(h)}$. *Then, $[r, s]$ is rewritable and it is detected by the F_5 criteria.*

Proof. Notice wlog, we can suppose that $max_{\prec}\{um\mathbf{f}_i, vm'\mathbf{f}_j\} = um\mathbf{f}_i$. Note with these assumptions, our results will be in terms of r and f. Let $\operatorname{Spoly}(f, h) = u'f - v'h$ and $\operatorname{Spoly}(g, h) = u''g - v''h$. Therefore, from [2], Proposition 5.70 page 223, we can write (for simplification we do not care about the coefficients)

$$\begin{aligned}
\operatorname{Spoly}(f, g) &= uf - vg \\
&= \frac{\operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(g))}{\operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(h))}u'f - \frac{\operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(g))}{\operatorname{lcm}(\operatorname{LM}(g), \operatorname{LM}(h))}v'g \\
&= \frac{\operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(g))}{\operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(h))}(u'f - v'h) - \frac{\operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(g))}{\operatorname{lcm}(\operatorname{LM}(g), \operatorname{LM}(h))}(u''g - v''h) \\
&= \frac{\operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(g))}{\operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(h))}\operatorname{Spoly}(f, h) - \frac{\operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(g))}{\operatorname{lcm}(\operatorname{LM}(g), \operatorname{LM}(h))}\operatorname{Spoly}(g, h).
\end{aligned}$$

From the hypothesis, we can conclude that $\mathcal{S}(\operatorname{Spoly}(r, t)) = u'm\mathbf{f}_i$. Otherwise, we have $u'm\mathbf{f}_i \prec v'm''\mathbf{f}_\ell$, and multiplying both sides of this inequality by $\frac{\operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(g))}{\operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(h))}$, we obtain $um\mathbf{f}_i \prec wm''\mathbf{f}_\ell$, which is a contradiction. Now, using the above equalities we show that $[r, s]$ is rewritable. We have $u'm > m$ and $u'm \mid um$. Therefore, $[r, s]$ is rewritable by $\operatorname{Spoly}(r, t)$, and this ends the proof. □

Corollary 3.2. *With the notations of Lemma 3.4, assume that* $\operatorname{LM}(h)$ *divides* $\operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(g))$ *and both the pairs (r, t) and (s, t) have already been treated. If* $\max_{\prec}\{um\mathbf{f}_i, vm'\mathbf{f}_j\} \prec wm''\mathbf{f}_\ell$ *then (r, s) is a useless pair and it may not be detected by the F_5 criteria.*

It is worth noting that if the input polynomial system is a regular sequence, then there is no reduction to zero during the execution of the F_5 algorithm (see [8], Corollary 3). Therefore, the conditions of the above corollaries are not satisfied for any critical pair in this case.

4. Description of the new algorithm

In this section, we present our algorithm to compute the Gröbner basis of an ideal. This algorithm is designed such that it uses the IsRewritten criterion with Buchberger's criteria. We first describe the F5Buchberger algorithm which has a structure similar to the GröbnerNew2 algorithm (see [2] page 232). The latter algorithm is a generalization of the Buchberger algorithm by applying Buchberger's criteria (throughout this paper, we call it the Buchberger algorithm). Before it, we introduce a new module monomial ordering on the signatures, and also a new selection strategy that we use in our algorithm. Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring, where K is an arbitrary field, let $I = \langle f_1, \ldots, f_k\rangle$ be an ideal of R and let $<$ be a monomial ordering on R.

Definition 4.1. We define $m_1\mathbf{f_{i_1}} \prec_N m_2\mathbf{f_{i_2}}$ if

$$\begin{cases} \deg(m_1 f_{i_1}) < \deg(m_2 f_{i_2}) \text{ or} \\ \deg(m_1 f_{i_1}) = \deg(m_2 f_{i_2}) \text{ and } i_2 < i_1 \text{ or} \\ \deg(m_1 f_{i_1}) = \deg(m_2 f_{i_2}) \text{ and } i_1 = i_2 \text{ and } m_1 < m_2. \end{cases}$$

In our algorithm, we present a new selection strategy (which has a good performance in practice, see Section 6), comparing the critical pairs considering priority to a lower signature (using the above ordering) of corresponding S-polynomials, and breaking ties with another strategy which considers priority to the older constructed pairs: We say the pair (r_{i_1}, r_{i_2}) is older than (r_{j_1}, r_{j_2}) if $\max\{i_1, i_2\} < \max\{j_1, j_2\}$ or $\max\{i_1, i_2\} = \max\{j_1, j_2\}$ and $\min\{i_1, i_2\} > \min\{j_1, j_2\}$. We refer to this new strategy as the *$\mathcal{S}$-position* strategy. The idea of this strategy is due to the Gebauer and Möller algorithm (see [2] pages 230–232): When there is a Buchberger triple (f, g, h), i.e. $\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g)) = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(h))$, the algorithm chooses the former constructed pair between (f, g) and (f, h) for deletion. That is why we use this strategy in the $\mathcal{S}$-position, for the compatibility of the IsRewritten criterion and Buchberger's criteria.

It is worth noting that the $\mathcal{S}$-position strategy may be considered as a generalization of the *sugar strategy* (see the following lemma). By the sugar strategy, the pairs are ordered with respect to a phantom degree called sugar. For the input polynomials f_i, we define $\deg_s(f_i) = \deg(f_i)$ for each i. If f is a polynomial and m is a term, then $\deg_s(m.f) = \deg(m) + \deg_s(f)$. Finally, if f and g are two polynomials, $\deg_s(f + g) = \max\{\deg_s(f), \deg_s(g)\}$. For a critical pair (f, g), we define its sugar degree to be the sugar of $\mathrm{Spoly}(f, g)$. The sugar strategy chooses a pair with a minimal sugar degree (see [11] for more details).

Lemma 4.1. *Let $r = (m\mathbf{f_i}, f)$ be an admissible labeled polynomial. Then, the degree of $m\mathbf{f_i}$ (which is defined to be $\deg(m) + \deg(f_i)$) is equal to $\deg_s(f)$.*

Proof. If $r = (\mathbf{f_i}, f_i)$, then the assertion is trivial. According to the structure of F5Buchberger's algorithms (Algorithm 1), it is enough to prove that if $r = (m\mathbf{f_i}, f)$ is the S-polynomial of (r_1, r_2) for some $r_1 = (m_1\mathbf{f_{i_1}}, g_1)$ and $r_2 = (m_2\mathbf{f_{i_2}}, g_2)$ with $\deg(m_1\mathbf{f_{i_1}}) = \deg_s(g_1)$ and $\deg(m_2\mathbf{f_{i_2}}) = \deg_s(g_2)$ then $\deg(m\mathbf{f_i}) = \deg_s(f)$. From the definition of the S-polynomial, we have $m\mathbf{f_i} = \max_{\prec_N}\{u_1 m_1\mathbf{f_{i_1}}, u_2 m_2\mathbf{f_{i_2}}\}$ where $u_t = \mathrm{lcm}(\mathrm{LM}(g_1), \mathrm{LM}(g_2))/\mathrm{LM}(g_t)$ for $t = 1, 2$. Since, $\prec_N$ is a degree ordering and $\deg(m_t\mathbf{f_{i_t}}) = \deg_s(g_t)$ for $t = 1, 2$, then $\deg(m\mathbf{f_i}) = \deg_s(f)$ by the definition of sugar degree. □

Algorithm 1 F5Buchberger

Require: $f_1, \ldots, f_k$; a list of polynomials and $<$; a monomial ordering
Ensure: A Gröbner basis of the ideal generated by $f_1, \ldots, f_k$ for $<$

```
Grob:= {}
Crtp:= {}
M:= {(f_i, f_i), 1 ≤ i ≤ k}
for r ∈ M do
  Grob , Crtp:=Update(Grob,Crtp,r)
end for
while Crtp ≠ ∅ do
  select and remove the smallest pair P (for S-position) from Crtp
  s:=Reduction(Spoly(P) , Grob)
  if poly(s)≠ 0 then
    Grob , Crtp:=Update(Grob,Crtp,s)
  end if
end while
Return {poly(r) | r ∈ Grob}
```

The algorithm UPDATE (Algorithm 2), updates the lists of critical pairs using a given polynomial, the IsRewritten criterion and Buchberger's criteria.

Algorithm 2 UPDATE

Require: Grob; the last computed basis, Crtp; a set of critical pairs, and r; an admissible labeled polynomial
Ensure: A set of labeled polynomials and a set of critical pairs
$C := \{\{r, s\} \mid s \in \text{Grob}\}$
$D := \emptyset$
while $C \neq \emptyset$ **do**
select and remove $\{r, s\}$ from C
if LM(poly(r)) and LM(poly(s)) are disjoint or
LM(poly(t)) $\nmid$ lcm(LM(poly(r)), LM(poly(s))) or
IsRewritten(r, s, t)=false for all $\{r, t\} \in C \cup D$ **then**
$D := D \cup \{\{r, s\}\}$
end if
end while
$E := \emptyset$
while $D \neq \emptyset$ **do**
select and remove $\{r, s\}$ from D
if LM(poly(r)) and LM(poly(s)) are not disjoint **then**
$E := E \cup \{\{r, s\}\}$
end if
end while
$B_{new} := E$
while Crtp$\neq \emptyset$ **do**
select and remove $\{s, t\}$ from Crtp
if (LM(poly(r)) $\nmid$ lcm(LM(poly(s)), LM(poly(t))) or
lcm(LM(poly(r)), LM(poly(s))) = lcm(LM(poly(s)), LM(poly(t))) or
lcm(LM(poly(r)), LM(poly(t))) = lcm(LM(poly(s)), LM(poly(t)))) and
IsRewritten(s, t, r)=false **then**
$B_{new} := B_{new} \cup \{\{s, t\}\}$
end if
end while
$G_{new} := \{r\}$
while Grob$\neq \emptyset$ **do**
select and remove s from Grob
if LM(poly(r)) $\nmid$ LM(poly(s)) **then**
$G_{new} := G_{new} \cup \{\{s\}\}$
end if
end while
Return(G_{new}, B_{new})

Algorithm 3 computes the S-polynomial of a critical pair of labeled polynomials.

Algorithm 3 SPOLY

Require: r, s; two admissible labeled polynomials
Ensure: The S-polynomial of (r, s)
$u := \frac{\text{lcm}(\text{LM}(\text{poly}(r)),\text{LM}(\text{poly}(s)))}{\text{LM}(\text{poly}(r))}$
$v := \frac{\text{lcm}(\text{LM}(\text{poly}(r)),\text{LM}(\text{poly}(s)))}{\text{LM}(\text{poly}(s))}$
$sp := u\text{LC}(s)\text{poly}(r) - v\text{LC}(r)\text{poly}(s)$
Return $(max_{\prec_N}\{u\mathcal{S}(r), v\mathcal{S}(s)\}, sp)$

We now present the IsREWRITTEN algorithm (Algorithm 4) which tests the IsRewritten criterion with some additional conditions (see Theorem 5.1).

Algorithm 4 IsRewritten

Require: $r = (m\mathbf{f_i}, f), s = (m'\mathbf{f_j}, g), t = (m''\mathbf{f}_\ell, h)$; three admissible labeled polynomials
Ensure: true if (r, s) is rewritable by t and false otherwise
$u := \frac{\text{lcm}(\text{LM}(f),\text{LM}(g))}{\text{LM}(f)}$
$v := \frac{\text{lcm}(\text{LM}(f),\text{LM}(g))}{\text{LM}(g)}$
if $i = \ell$ and $\mathcal{S}(r) \prec_N \mathcal{S}(t) \prec_N \mathcal{S}(s)$ and $m'' \mid um$ and $\mathcal{S}(\text{Spoly}(t, s)) \prec_N \mathcal{S}(\text{Spoly}(r, s))$ or
$j = \ell$ and $\mathcal{S}(s) \prec_N \mathcal{S}(t) \prec_N \mathcal{S}(r)$ and $m'' \mid vm'$ and $\mathcal{S}(\text{Spoly}(t, r)) \prec_N \mathcal{S}(\text{Spoly}(r, s))$ **then**
  Return true
else
  Return false
end if

We finally present an algorithm (Algorithm 5) to reduce a labeled polynomial w.r.t. the last computed basis.

Algorithm 5 Reduction

Require: r; a labeled polynomial and Grob; the last computed basis
Ensure: The reduced form of r w.r.t. Grob
while there exists $s \in$ Grob s.t. LM(poly(s)) | LM(poly(r)) **do**
  if $\frac{\text{LM}(\text{poly}(r))}{\text{LM}(\text{poly}(s))}\mathcal{S}(s) \prec_N \mathcal{S}(r)$ **then**
    $r :=$Spoly(r, s)
  end if
end while
Return r

5. Proof of the algorithm

In this section, we state our main result on combining the IsRewritten criterion with Buchberger's criteria. This result naturally yields the correctness of the F5Buchberger algorithm. Before that, we give an example which shows the nontriviality of our contribution and illustrates the difficulties in combining these criteria.

Example 5.1. In this example, we show two problems arising from combination of the IsRewritten criterion with Buchberger's criteria. Let

$$\begin{aligned} I = \langle & 10x_1^2x_4 + 10x_2^2x_4 + 10x_3^2x_4 - 11x_4h^2 + 10h^3, \\ & 10x_1^2x_3 + 10x_2^2x_3 + 10x_3x_4^2 - 11x_3h^2 + 10h^3, \\ & 10x_1x_2^2 + 10x_1x_3^2 + 10x_1x_4^2 - 11x_1h^2 + 10h^3, \\ & 10x_1^2x_2 + 10x_2x_3^2 + 10x_2x_4^2 - 11x_2h^2 + 10h^3\rangle \end{aligned}$$

be Noon4 ideal in $\mathbb{Q}[x_1, x_2, x_3, x_4, h]$ and let $<$ be the degree reverse lexicographical ordering with $x_1 > x_2 > x_3 > x_4 > h$. Let us denote by r_i the i-th computed polynomial for calculating a Gröbner basis of I. Then, $r_1, \ldots, r_4$ are the generators of I. We resume in the following some parts of the computation of the Gröbner basis of I. It is remarkable that we represent any computed polynomial only by its S-polynomial, and not by its reduced form (by this representation, some computations may seem wrong, however, our aim is to explain only the ideas). Let

- $r_5 := \text{Spoly}(r_1, r_2) = x_3r_1 - x_4r_2$ and $\mathcal{S}(r_5) = x_3\mathbf{f_1}$
- $r_6 := \text{Spoly}(r_1, r_4) = x_2r_1 - x_4r_4$ and $\mathcal{S}(r_6) = x_2\mathbf{f_1}$
- $r_7 := \text{Spoly}(r_2, r_4) = x_2r_2 - x_3r_4$ and $\mathcal{S}(r_7) = x_2\mathbf{f_2}$
- $r_8 := \text{Spoly}(r_3, r_4) = x_1r_3 - x_2r_4$ and $\mathcal{S}(r_8) = x_1\mathbf{f_3}$
- $r_9 := \text{Spoly}(r_2, r_8) = x_3r_2 + r_8$ and $\mathcal{S}(r_9) = x_3\mathbf{f_2}$
- $\text{Spoly}(r_5, r_9) = x_2^2r_5 + 1/2x_3x_4r_9$ and $x_2^2\mathcal{S}(r_5) = x_2^2x_3\mathbf{f_1}$ which is divisible by $\mathcal{S}(r_6)$. This follows that the pair (r_5, r_9) is rewritable and we can write:

$$\begin{aligned} \text{Spoly}(r_5, r_9) &= x_2^2r_5 + 1/2x_3x_4r_9 \\ &= x_2^2(x_3r_1 - x_4r_2) + 1/2x_3x_4r_9 \\ &= (x_2x_3r_6 + x_2x_3x_4r_4) - x_2^2x_4r_2 + 1/2x_3x_4r_9 \\ &= x_2x_3r_6 + x_2x_4\text{Spoly}(r_2, r_4) + 1/2x_3x_4r_9 \\ &= x_2x_3r_6 + x_2x_4r_7 + 1/2x_3x_4r_9 \end{aligned}$$

$$= x_2\text{Spoly}(r_6, r_7) + 1/2x_3x_4r_9 + 2x_2x_4r_7$$
$$= x_2^2r_5 + 1/2x_3x_4r_9 + 2x_2x_4r_7$$
$$= \text{Spoly}(r_5, r_9) + 2x_2x_4r_7.$$

Note that the reason to conclude the third line from the second one is that, $x_2^2r_5$ is rewritable by r_6, i.e. using the definition of r_6 we have $x_2x_3r_6 = x_2^2x_3r_1 - x_2x_3x_4r_4$, and from this we can replace $x_2^2x_3r_1$ by another expression containing r_6. The first problem is a (wrong) use of the IsRewritten criterion in $\text{Spoly}(r_5, r_9)$. Indeed, if we replace $x_2^2r_5$ by some multiplications of r_2, r_4, r_6 then this may re-produce r_5 by a different way which makes a loop.

Now, we study another problem. Let

- $r_{10} := \text{Spoly}(r_7, r_9) = x_3r_7 + 1/2x_2r_9$, $\mathcal{S}(r_{10}) = x_2x_3\mathbf{f_2}$, $\text{LM}(r_{10}) = x_2x_3^4$
- $r_{11} := \text{Spoly}(r_3, r_9) = x_3^2r_3 - 1/2x_1r_9$, $\mathcal{S}(r_{11}) = x_1x_3\mathbf{f_2}$, $\text{LM}(r_{11}) = x_3^4x_1$
- $r_{12} := \text{Spoly}(r_3, r_6) = x_2x_4r_3 + x_1r_6$, $\mathcal{S}(r_5) = x_1x_2\mathbf{f_1}$, $\text{LM}(r_{12}) = x_1x_2x_3^2x_4$
- $\text{Spoly}(r_{10}, r_{12}) = 1/2x_1x_4r_{10} + x_3^2r_{12}$. Since $x_1x_4\mathcal{S}(r_{10}) = x_1x_2x_3x_4\mathbf{f_2}$ is divisible by $\mathcal{S}(r_{11})$ then the pair (r_{10}, r_{12}) is rewritable and we can write:

$$\begin{aligned}\text{Spoly}(r_{10}, r_{12}) &= 1/2x_1x_4r_{10} + x_3^2r_{12}\\ &= 1/2x_1x_4(x_3r_7 + 1/2x_2r_9) + x_3^2r_{12}\\ &= 1/2x_1x_4(x_3(x_2r_2 - x_3r_4) + 1/2x_2r_9) + x_3^2r_{12}\\ &= 1/2x_1x_2x_3x_4r_2 - 1/2x_1x_3^2x_4r_4 + 1/4x_1x_2x_4r_9 + x_3^2r_{12}\\ &= x_2x_3^2x_4r_3 - 1/2x_1x_2x_4r_8 - x_2x_4r_{11} - 1/2x_1x_3^2x_4r_4 + 1/4x_1x_2x_4r_9 + x_3^2r_{12}\\ &= \text{Spoly}(r_{11}, r_{12}) + x_2x_3^2x_4r_3 - 1/2x_1x_2x_4r_8 - 2x_2x_4r_{11} - 1/2x_1x_3^2x_4r_4 + 1/4x_1x_2x_4r_9.\end{aligned}$$

Note that the reason behind writing the fifth line from the fourth is that, using definition of r_{11} we have $r_{11} = x_3^2r_3 - 1/2x_1(x_3r_2 + r_8) = -1/2x_1x_3r_2 + x_3^2r_3 - 1/2x_1r_8$ and we can replace $1/2x_1x_2x_3x_4r_2$ by another expression. Now, since, $\text{LM}(r_{10}) \mid \text{lcm}(\text{LM}(r_{11}), \text{LM}(r_{12}))$ then we eliminate the pair (r_{11}, r_{12}) if we are sure to study the pairs (r_{10}, r_{11}) and (r_{10}, r_{12}). On the other hand, we omit (r_{10}, r_{12}) by the IsRewritten criterion referring to study the pair (r_{11}, r_{12}), and this makes a loop. Remark that $\text{LM}(r_{11}) \mid \text{lcm}(\text{LM}(r_{10}), \text{LM}(r_{12}))$, and therefore (r_{12}, r_{10}, r_{11}) forms a Buchberger triple, and Buchberger's algorithm removes the pair (r_{10}, r_{12}) and keeps the pair (r_{11}, r_{12}).

Now, we state the main theorem of this paper.

Theorem 5.1. *Let $I = \langle f_1, \ldots, f_k\rangle \subset R$ be an ideal. Let r_i, r_j and r_m be three admissible labeled polynomials treated during a run of* F5Buchberger *algorithm for computing a Gröbner basis of I. Let $u_s = \frac{\text{lcm}(\text{LM}(\text{poly}(r_i)), \text{LM}(\text{poly}(r_j)))}{\text{LM}(\text{poly}(r_s))}$ for $s \in \{i, j\}$. If*

- $\mathcal{S}(r_i) \prec_N \mathcal{S}(r_m) \prec_N \mathcal{S}(r_j)$
- *$[u_i, r_i]$ is rewritable by r_m*
- $\mathcal{S}(\text{Spoly}(r_m, r_j)) \prec_N \mathcal{S}(\text{Spoly}(r_i, r_j))$

then $\text{Spoly}(r_i, r_j)$ is either zero or equal to $o_G(u_sr_s)$ for $s \in \{1, 2\}$ (and therefore the pair (r_i, r_j) can be eliminated).

Proof. Let $\text{Spoly}(r_i, r_j) \neq 0$. From hypothesis $[u_i, r_i]$ is rewritable, hence we can replace u_ir_i by (1) in $\text{Spoly}(r_i, r_j) = u_ir_i + u_jv_j$. In the new expression the two following cases may be take place:

- Let r_j and r_m form an S-polynomial. Since $\mathcal{S}(\text{Spoly}(r_m, r_j)) \prec_N \mathcal{S}(\text{Spoly}(r_i, r_j))$, the pair (r_m, r_j) has been treated before (r_i, r_j) (see $\mathcal{S}$-position strategy). Thus, it has a standard representation, and $\text{Spoly}(r_i, r_j)$ is equal to $o_G(u_sr_s)$ for $s \in \{1, 2\}$.
- If r_j and r_m do not form an S-polynomial, an S-polynomial can be formed between r_j and r_t where r_t is an admissible labeled polynomial in (1). Note that this polynomial may be also the result of some S-polynomials in (1). Thus, we can write $u_tr_t + u_jr_j = u\text{Spoly}(r_t, r_j)$ where u and u_t are two monomials such that $u_j\text{LM}(\text{poly}(r_j)) = u_t\text{LM}(\text{poly}(r_t))$. This yields $\text{LM}(\text{poly}(r_t)) \mid \text{lcm}(\text{LM}(\text{poly}(r_i)), \text{LM}(\text{poly}(r_j)))$. Here two cases are possible:
  - If $u \neq 1$, then $\mathcal{S}(\text{Spoly}(r_t, r_j)) \prec_N \mathcal{S}(\text{Spoly}(r_i, r_j))$. Thus, (r_t, r_j) has been treated before the pair (r_i, r_j), and it has a standard representation.
  - If $u = 1$, then

    $$\text{lcm}(\text{LM}(\text{poly}(r_i)), \text{LM}(\text{poly}(r_j))) = \text{lcm}(\text{LM}(\text{poly}(r_t)), \text{LM}(\text{poly}(r_j)))$$

    and therefore (r_j, r_i, r_t) forms a Buchberger triple. We now consider the pair (r_t, r_j). The only case that may create a loop, is the case that $[u_t, r_t]$ is rewritable by an admissible labeled polynomial r_s and u_ir_i appears in the new form of $\text{Spoly}(r_t, r_j)$. We study this case in the following. From rewritability of $[u_t, r_t]$, we have $\mathcal{S}(r_t) \prec_N \mathcal{S}(r_j)$ and we can also replace u_tr_t by another expression (containing u_ir_i) like (1) in $\text{Spoly}(r_t, r_j) = u_tr_t + u_jr_j$. Since u_ir_i appears in u_tr_t, then r_t must be the result of the S-polynomial of r_m and another admissible labeled polynomial. This follows $\mathcal{S}(r_i) \prec_N \mathcal{S}(r_t)$. In this case, (r_i, r_j) is older than (r_t, r_j) and Update algorithm deletes (r_i, r_j) and holds (r_t, r_j). Thus, (r_t, r_j) has a standard representation. □

6. Experiments and results

We have implemented the F5Buchberger and Buchberger algorithms in Ma-ple 12. The first algorithm corresponds to the implementation of our algorithm, and the second one is the Gebauer and Möller algorithm (see [2] pages 230–232) using the sugar-normal selection strategy.

For these experiments, we used some examples from the Posso list[1]. The results are shown in the following tables where the timings were conducted on a personal computer with 3.2 GHz, a 2×Intel(R)-Xeon(TM) Quad core, 24 GB RAM and 64 bits under the Linux operating system. In these tables, the first column denotes the algorithm. The "time" column shows the CPU time in seconds consumed by the corresponding algorithm. The "memory" column lists the amount of gigabytes of memory used by the algorithm. The "reds." column counts the number of reductions to zero. The "Buch1/2" column presents the number of critical pairs satisfying Buchberger's criteria, detected by the corresponding algorithm. The "IsR." column contains the number of critical pairs satisfying IsRewritten criterion (detected by the F5Buchberger algorithm). The "nb." column gives the number of polynomials computed in the output basis. The "reduced" column shows the CPU time in seconds consumed to compute the reduced Gröbner basis from the Gröbner basis computed by the corresponding algorithm. The $\mathbb{Z}_p$ column lists the CPU time in seconds consumed to compute a Gröbner basis over the field $\mathbb{Z}_p$ for $p = 2147483647$ (the biggest prime number less than 2^{31}). All the computations are done over $\mathbb{Q}$ (except $\mathbb{Z}_p$ column) and the monomial ordering is degree reverse lexicographical ordering.

The experiments we performed seem to show that this first implementation of F5Buchberger is already very efficient. Although, for some examples, it is less efficient than Buchberger, but a comparison of the timing columns in the above tables and our test for about 50 examples show that the new algorithm is more stable and more efficient than Buchberger.

It is worth noting that according to this special type of reduction (see Reduction algorithm), used in F5Buchberger:

- we had to write the reduction algorithm for Buchberger, and we could not use the `NormalForm` function from the Groebner package of Maple. Thus the timing data are not to be expected.
- the number of critical pairs and elements of Gröbner basis computed by F5Buchberger is greater than Buchberger. Therefore, the comparison of the reds. column may not be a good indicator.

Schrans-Troost	time	memory	reds.	Buch.1/2	IsR.	reduced	nb.	$\mathbb{Z}_p$
F5Buchberger	8933	74.744	585	8886	2436	47.95	183	5899
Buchberger	38784	375.781	652	7356	-	13.56	128	13563

Cyclic6	time	memory	reds.	Buch.1/2	IsR.	reduced	nb.	$\mathbb{Z}_p$
F5Buchberger	909.41	4.854	259	14712	3989	3.92	157	152.34
Buchberger	1495.57	19.132	344	4699	-	0.31	45	247.13

Eco8	time	memory	reds.	Buch.1/2	IsR.	reduced	nb.	$\mathbb{Z}_p$
F5Buchberger	750.66	4.434	263	4142	341	8.28	87	606.49
Buchberger	686.46	5.451	264	1985	-	0.62	59	504.38

Chemkin	time	memory	reds.	Buch.1/2	IsR.	reduced	nb.	$\mathbb{Z}_p$
F5Buchberger	716.19	5.178	398	8897	989	7.49	159	476.76
Buchberger	2781.24	36.055	403	3095	-	1.00	85	905.24

Huneke	time	memory	reds.	Buch.1/2	IsR.	reduced	nb.	$\mathbb{Z}_p$
F5Buchberger	111.13	0.851	262	12505	2257	3.51	175	147.43
Buchberger	178.18	1.944	279	4977	-	1.74	104	204

Eco7	time	memory	reds.	Buch.1/2	IsR.	reduced	nb.	$\mathbb{Z}_p$
F5Buchberger	25.82	0.212	109	838	50	0.42	43	28.21
Buchberger	32.41	0.318	111	508	-	0.08	32	32.53

Vermeer	time	memory	reds.	Buch.1/2	IsR.	reduced	nb.	$\mathbb{Z}_p$
F5Buchberger	20.76	0.164	83	1572	217	0.15	33	28.02
Buchberger	31.06	0.319	90	731	-	0.06	20	30.87

[1] The Maple code of our programs and examples are available at: http://amirhashemi.iut.ac.ir/software.html.

Cyclic5	time	memory	reds.	Buch.1/2	IsR.	reduced	nb.	$\mathbb{Z}_p$
F5Buchberger	2.85	0.022	69	557	126	0.05	28	3.32
Buchberger	5.73	0.054	81	527	-	0.02	20	5.83

Noon4	time	memory	reds.	Buch.1/2	IsR.	reduced	nb.	$\mathbb{Z}_p$
F5Buchberger	2.73	0.022	46	303	19	0.14	31	4.04
Buchberger	4.26	0.040	47	307	-	0.10	28	4.90

Haas3	time	memory	reds.	Buch.1/2	IsR.	reduced	nb.	$\mathbb{Z}_p$
F5Buchberger	2.41	0.019	118	2133	302	0.13	64	3.35
Buchberger	4.52	0.038	124	1906	-	0.12	57	4.60

Liu	time	memory	reds.	Buch.1/2	IsR.	reduced	nb.	$\mathbb{Z}_p$
F5Buchberger	0.86	0.007	18	30	1	0.01	13	1.20
Buchberger	1.36	0.012	18	40	-	0.01	12	1.56

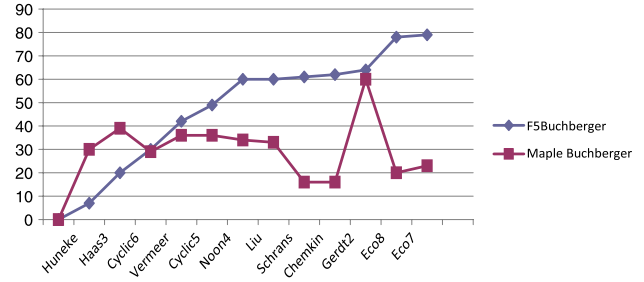
Gerdt2	time	memory	reds.	Buch.1/2	IsR.	reduced	nb.	$\mathbb{Z}_p$
F5Buchberger	0.33	0.002	4	17	0	0.02	8	0.50
Buchberger	0.48	0.004	4	18	-	0.02	8	0.59

Finally, to show the usefulness of our algorithm, we have used the verbose options of Maple as follows. The commands

```
with(Groebner);
infolevel[Basis]:=3;
Basis(G,T,method=buchberger);
```

compute (using Buchberger's algorithm equipped with the Update algorithm) the reduced Gröbner basis of G w.r.t. T with some extra information. For example, it shows the number of useful critical pairs and reductions to zero. By an useful critical pair, we mean a pair whose S-polynomial does not reduce to zero, and by a reduction to zero, we mean a non useful critical pair which is not detected by Buchberger's criteria. In the following table (and its diagram), we compare the usefulness of F5Buchberger with the function `Basis` of Maple using Buchberger's method (we call this function Maple Buchberger). Each row of this table shows the percent ratio of the number of useful critical pairs to the number of useful critical pairs plus the number of reductions to zero, for the corresponding algorithm.

Examples	F5Buchberger	Maple Buchberger
Huneke	7	30
Haas3	20	39
Cyclic6	30	29
Vermeer	42	36
Cyclic5	49	36
Noon4	60	34
Liu	60	33
Schrans	61	16
Chemkin	62	16
Gerdt2	64	60
Eco8	78	20
Eco7	79	23



Acknowledgements

The authors would like to thank Dr. Gwénolé Ars for fruitful discussions on the subject of this paper, and also the referees for their helpful comments. This work (for the first author) was supported in part by the CEAMA, Isfahan University of Technology, Isfahan 84156, Iran.

References

[1] G. Ars, A. Hashemi, Extended F_5 criteria, J. Symbolic Comput. 45 (12) (2010) 1330–1340.
[2] T. Becker, V. Weispfenning, Gröbner bases, in: Graduate Texts in Mathematics, vol. 141, Springer-Verlag, New York, 1993, (A computational approach to commutative algebra, In cooperation with Heinz Kredel).
[3] B. Buchberger, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nuildimensionalen Polynomideal, Ph.D. Thesis, Universität Innsbruck, 1965.
[4] B. Buchberger, A criterion for detecting unnecessary reductions in the construction of Gröbner-bases, in: Symbolic and Algebraic Computation (EUROSAM'79, Internat. Sympos., Marseille, 1979), in: Lecture Notes in Comput. Sci., vol. 72, Springer, Berlin, 1979, pp. 3–21.
[5] B. Buchberger, Gröbner bases: an algorithmic method in polynomial ideal theory, in: Recent Trends in Multidimensional Systems Theory, 1986, pp. 184–232.
[6] C. Eder, J. Perry, F5C: a variant of Faugère's F5 algorithm with reduced Gröbner bases, in: Effective Methods in Algebraic Geometry, 2009, pp. 32–33.
[7] J.-C. Faugère, A new efficient algorithm for computing Gröbner bases (F_4), J. Pure Appl. Algebra 139 (1–3) (1999) 61–88. (Effective methods in algebraic geometry (Saint-Malo, 1998)).
[8] J.-C. Faugère, A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5), ISSAC, ACM Press, 2002, 75–83.
[9] S. Gao, Y. Guan, F. Volny IV, A new incremental algorithm for computing Groebner bases, ISSAC, ACM Press, 2010, 13–19.
[10] R. Gebauer, H.M. Möller, On an Installation of Buchberger's Algorithm, J. Symbolic Comput. 6 (2–3) (1988) 275–286.
[11] A. Giovini, T. Mora, G. Niesi, L. Robbiano, C. Traverso, One Sugar Cube Please'' or Selection Strategies in Buchberger Algorithm, in: ISSAC, ACM Press, 1991, pp. 49–54.
[12] D. Lazard, Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations, in: Computer Algebra (London, 1983), in: Lecture Notes in Comput. Sci., vol. 162, Springer, Berlin, 1983, pp. 146–156.
[13] H.M. Möller, F. Mora, C. Traverso, Gröbner Bases Computation Using Syzygies, ISSAC, ACM Press, 1992, 320–328.
[14] Y. Sun, D. Wang, The F5 Algorithm in Buchberger's Style. Arxiv preprint arXiv:1006.5299, 2010.